Eindeutige Faktorisierung ohne ideale Elemente

Krause, Ulrich

Veröffentlicht in:
Abhandlungen der Braunschweigischen Wissenschaftlichen Gesellschaft Band 33, 1982, S.169-177

Verlag Erich Goltze KG, Göttingen

Eindeutige Faktorisierung ohne ideale Elemente

Von **Ulrich Krause,** Bremen

1. Extraktionsbereiche

In diesem Artikel wird versucht, für Bereiche, in denen eine global eindeutige Faktorisierung von Nichteinheiten in irreduzible Elemente nicht mehr möglich ist, dennoch eine Faktorisierung im Bereich selbst zu finden, die, auf noch zu erläuternde Weise, lokal eindeutig ist. Die geeigneten Bereiche dafür sind die unten definierten Extraktionsbereiche. Es zeigt sich, daß ein Bereich, der eine eindeutige Faktorisierung durch ideale Elemente erlaubt – d.h.: eine Divisorentheorie besitzt – auch ein Extraktionsbereich ist, daß es jedoch interessante Extraktionsbereiche gibt, die keine Divisorentheorie besitzen.

Unter einem (Teilbarkeits)**Bereich** S wird im folgenden immer eine kommutative (meistens multiplikative) Halbgruppe mit Einselement und Kürzungsregel verstanden. Ist R ein (kommutativer) Integritätsring mit 1, so ist $R^* = R\setminus\{0\}$ bzgl. Multiplikation ein solcher Bereich. Wie im Falle von Ringen bezeichnet $x \mid y$, daß $x \in S$ ein Teiler von $y \in S$ ist, U die Gruppe der Einheiten von S, $(x) = xS$ das von x erzeugte Ideal, $\mathrm{rad}(x) = \{y \in S \mid y^n \in (x) \text{ für ein } n \in \mathbb{N} \cup \{0\}\}$ das Radikal von (x) ($\mathbb{N} = \{1,2,\ldots\}$). Ist $x \in S$ eine Nichteinheit, so heißt x irreduzibel, wenn $x = y \cdot z$ impliziert, daß y oder z aus U ist; x heißt prim, wenn $x \mid y \cdot z$ impliziert, daß $x \mid y$ oder $x \mid z$; x heißt semiprim, wenn (x) semiprimes Ideal ist, d.h. $\mathrm{rad}(x) = (x)$.

Besonders durchsichtig ist die Teilbarkeitstheorie in einem **Gaußbereich,** d.h. einem Bereich S, in dem jede Nichteinheit eine eindeutige Faktorisierung, bis auf Einheiten und Reihenfolge der Faktoren, in irreduzible Elemente besitzt (vgl. [Kurös]). Aber bereits der einfache Gaußbereich $\mathbb{N}$ (bzgl. Multiplikation) enthält Bereiche S, deren Teilbarkeitsrelation mit der von $\mathbb{N}$ übereinstimmt, d.h. für $x,y \in S$ gilt $x \mid y$ genau dann, wenn $x \mid y$ gilt, die jedoch nicht gaußsch sind, z.B. $S = \{4n+1 \mid n \in \mathbb{N} \cup \{0\}\}$ (vgl. [Sommer]). Allgemein gilt, daß jeder Gaußbereich, der keine Gruppe ist, einen Bereich enthält, der nicht gaußsch ist ([Greiter]). Für die Untersuchung der Teilbarkeitseigenschaften in einem Bereich, der nicht gaußsch ist, erweist sich der folgende Extraktionsgrad als nützlich, der gewissermaßen den größten Anteil mißt, mit dem ein Element in einem anderen enthalten ist und daher aus diesem extrahiert werden kann. (Die im folgenden dargestellte Methode wurde ursprünglich in [Hinrichsen/Krause] für konvexe Mengen entwickelt, insbesondere zur simplizialen Zerlegung von Polyedern.)

Definition. Für einen Bereich S heißt die Abbildung

$$\lambda_S : S \times S \longrightarrow \mathbb{R}_+ \cup +\infty,\ \lambda_S(x,y) = \sup\left\{\tfrac{m}{n} \mid x^m \mid y^n \text{ mit } m,n \in \mathbb{N} \cup \{0\},\ n \neq 0\right\}$$

Extraktionsgrad in S. Gibt es für jedes Paar $x,y \in S$ mit $x \notin U$ ein Paar $m,n \in \mathbb{N} \cup \{0\}$ mit $n \neq 0$, so daß $x^m \mid_S y^n$ und $\lambda_S(x,y) = \frac{m}{n}$ ist, so heißt S **Extraktionsbereich.** Ist S ein Extraktionsbereich, so bezeichne für $x \in S \setminus U$, $y \in S$ $e(x,y)$ den durch $\lambda_S(x,y) = \frac{m}{n}$, $y^n = x^m \cdot z$ bei minimalem n eindeutig bestimmten Rest z, und $e: S \setminus U \longrightarrow S$ die dadurch definierte **Extraktionsfunktion.** Ist $\lambda_S(x,y) > 0$, so heißt x **Komponente** von y. Der Extraktionsgrad in einem Extraktionsbereich besitzt folgende elementare Eigenschaften.

Eigenschaften des Extraktionsgrades λ

(1) $(x) \subset \{y \in S \mid \lambda(x,y) \geqq 1\} \subset \{y \in S \mid \lambda(x,y) > 0\} = \mathrm{rad}(x)$
(2) $\lambda(x^k, y^l) = \frac{l}{k} \cdot \lambda(x,y)$ für $k,l \in \mathbb{N}$
(3) $\lambda(x_1 \cdot x_2, y) \leqq \min\{\lambda(x_1,y), \lambda(x_2,y)\}$
(4) $\lambda(x, y_1 \cdot y_2) \geqq \lambda(x,y_1) + \lambda(x,y_2)$
(5) x ist genau dann semiprim, wenn für alle $y \in S$ $\lambda(x,y) \in \mathbb{N} \cup \{0\}$ bzw. $\lambda(x,y) = \max\{m \in \mathbb{N} \cup \{0\} \mid x^m \mid y\}$.
(6) x ist genau dann prim, wenn x semiprim ist und für alle $y_1, y_2 \in S$ gilt $\lambda(x, y_1, y_2) = \lambda(x,y_1) + \lambda(x,y_2)$.

Offensichtlich ist $\mathbb{N}$ bezüglich der Multiplikation und $\mathbb{N} \cup \{0\}$ bezüglich der Addition ein Extraktionsbereich. Der folgende Satz liefert zwei Prinzipien, um aus Extraktionsbereichen, z. B. den eben genannten, weitere Extraktionsbereiche, z. B. Krullringe, zu gewinnen.

Satz 1

(a) Sei R ein Extraktionsbereich und S ein Unterbereich von R derart, daß zu $x,y \in S$ mit $x \mid_R y$ ein $k \in \mathbb{N}$ existiert mit $x^k \mid_S y^k$. Dann ist S ein Extraktionsbereich und die Extraktionsgrade von S und R stimmen auf SxS überein.
(b) Sei S ein Bereich, der Durchschnitt einer Familie $\{R_i\}_{i \in I}$ von Extraktionsbereichen (in einem Bereich R) ist, derart, daß jedes Element von S nur für endlich viele $i \in I$ eine Nichteinheit von R_i ist. Dann ist S ein Extraktionsbereich und für die Extraktionsgrade λ von S, λ_i von R_i gilt $\lambda(x,y) = \min\{\lambda_i(x,y) \mid x \text{ Nichteinheit von } R_i\}$ für $x,y \in S$.

Beweis:

(a) Seien $x,y \in S$. Es ist $\lambda_S(x,y) \leqq \lambda_R(x,y)$. Ist x Einheit in S, so $\lambda_S(x,y) = +\infty$ und es gilt Gleichheit. Ist x keine Einheit in S, so nach Voraussetzung auch keine Einheit in R. Da R Extraktionsbereich, so folgt $\lambda_R(x,y) = \frac{m}{n}$ und $x^m \mid_R y^n$. Nach Voraussetzung gibt es ein $k \in \mathbb{N}$ mit $x^{mk} \mid_S y^{nk}$, und es ist $\lambda_S(x,y) \geqq \frac{mk}{nk} = \lambda_R(x,y) \geqq \lambda_S(x,y)$.
(b) Seien $x,y \in S$ und $\tilde{I} = \{i \in I \mid x \text{ Nichteinheit in } R_i\}$. Da $S \subset R_i$ für $i \in I$, so $\lambda_S(x,y) \leqq \leqq \min\{\lambda_i(x,y) \mid i \in \tilde{I}\}$. Wegen $S = \bigcap_{i \in I} R_i$ ist x Einheit in S genau dann, wenn x Einheit in allen R_i ist. Ist also x Einheit in S, so $\lambda_S(x,y) = +\infty = \min\{\lambda_i(x,y) \mid i \in \tilde{I}\}$. Ist x Nichteinheit in S, so ist $\tilde{I} \neq \emptyset$. Für $i \in \tilde{I}$ gibt es m_i, n_i mit $\lambda_i(x,y) = \frac{m_i}{n_i}$ und $y^{n_i} = x^{m_i} \cdot z_i, z_i \in R_i$, da R_i Extraktionsbereich ist. Sei

$\frac{m_j}{n_j} = \min\{\frac{m_i}{n_i} \mid i \in \tilde{I}\}$. Dann
$y^{n_i n_j} = x^{m_i n_j} \cdot z_i^{n_j}$, $y^{n_j n_i} = x^{m_j n_i} \cdot z_j^{n_i}$ und wegen
$m_j \cdot n_i \leqq m_i \cdot n_j$ ist $x^{m_i n_j - m_j n_i} \cdot z_i^{n_j} = z_j^{n_i}$.

Da $x \in S$, $z_i \in R_i$, so $z_j^{n_i} \in R_i$ für alle $i \in \tilde{I}$. Ist $n = \prod_{i \in \tilde{I}} n_i$, so $z_j^n \in R_i$ für $i \in \tilde{I}$. Für $i \in I$, $i \notin \tilde{I}$ ist x Einheit in R_i und wegen $y^{n_j n} = x^{m_j n} \cdot z_j^n$ daher $z_j^n \in R_i$ für $i \notin \tilde{I}$. Also ist $z_j^n \in S$ und daher $x^{m_j n} \mid_S y^{n_j n}$ und $\lambda_S(x,y) \geqq \frac{m_j n}{n_j n} = \min\{\lambda_i(x,y) \mid i \in \tilde{I}\} \geqq \lambda_S(x,y)$.

Folgerungen

(1) Sei $h: S \longrightarrow R$ ein Halbgruppenhomomorphismus der Bereiche S und R mit $h(x) \mid_R h(y) \Leftrightarrow x \mid_S y$ für $x,y \in S$. Dann ist mit R auch S ein Extraktionsbereich und $\lambda_S(x,y) = \lambda_R(h(x),h(y))$ für $x,y \in S$ (nach Satz 1 (a)).
Beispiel: Sei R ein Bewertungsring zu einer diskreten Bewertung ν. ν induziert einen Halbgruppenhomomorphismus des Bereiches R^* in den Extraktionsbereich $\mathbb{N} \cup \{0\}$ (bzgl. Addition) mit $x \mid_{R^*} y \Leftrightarrow \nu(x) \leqq \nu(y)$. Also ist R^* ein Extraktionsbereich und $\lambda_{R^*}(x,y) = \frac{\nu(y)}{\nu(x)}$ für $x,y \in R^*$, da $\lambda_{\mathbb{N}\cup\{0\}}(k,l) = \frac{l}{k}$ (mit $\frac{0}{0} = +\infty$). (Der Zusammenhang zwischen λ_{R^*} und ν ist so eng, daß man einen diskreten Bewertungsring durch Eigenschaften seines Extraktionsgrades charakterisieren kann.)

(2) Ist R ein Krullring, so ist R^* ein Extraktionsbereich und $\lambda_{R^*}(x,y) = \min\{\frac{\nu_i(y)}{\nu_i(x)} \mid \nu_i(x) > 0, i \in I\}$, wobei $(\nu_i)_{i \in I}$ definierende Familie diskreter Bewertungen von R.
(Folgt aus Satz 1 (b) und Beispiel unter Folgerung (1).) Insbesondere sind also Gaußsche Ringe (faktorielle Ringe) und Dedekindsche Ringe Extraktionsbereiche.

(3) Sei S ein Bereich mit Divisorentheorie, d.h. es gibt einen Halbgruppenhomomorphismus $h: S \longrightarrow G$ in einen Gaußbereich G mit $x \mid_S y \Leftrightarrow h(x) \mid_G h(y)$ (vgl. [Gundlach]). Da ein Gaußbereich, analog wie ein Gaußring, ein Extraktionsbereich ist, so folgt aus Folgerung (1), daß S ein Extraktionsbereich ist mit $\lambda_S(x,y) = \lambda_G(h(x), h(y))$. Insbesondere ist also ein Unterbereich eines Gaußbereiches G, dessen Teilbarkeitsrelation mit der von G übereinstimmt, ein Extraktionsbereich.

(4) Sei R ein Krullring und S ein Unterbereich von R^* derart, daß für jedes Element von R^* eine Potenz in S liegt. Dann ist S ein Extraktionsbereich, λ_S und λ_{R^*} stimmen auf SxS überein. (Folgt aus Satz 1 (a) und Folgerung (2).) Im allgemeinen ist ein Unterring S eines Krullringes mit obiger Eigenschaft nicht selbst wieder ein Krullring, wie etwa das Beispiel $R = \mathbb{Z}(\sqrt{-5})$, $S = \mathbb{Z} + 2\mathbb{Z} \cdot \sqrt{-5}$ zeigt. $\mathbb{Z} + 2\mathbb{Z} \cdot \sqrt{-5}$ ist ein Extraktionsbereich, besitzt aber als Nicht-Hauptordnung keine Divisorentheorie.

Bemerkung. Indem man für einen Bereich die zugehörige Quotientengruppe betrachtet, kann man ähnlich wie im Fall von Ringen Bewertungen, Bewertungsbereiche und Krullbereiche definieren. Die obigen Folgerungen gelten dann ganz analog für diese etwas allgemeinere Situation.

2. Markierte Faktorisierungen

Sei S ein Extraktionsbereich mit Extraktionsgrad $\lambda = \lambda_S$ und S bestehe nicht nur aus Einheiten. Die Extraktion von Elementen, beschrieben durch die Extraktionsfunktion $e(\cdot,\cdot)$, läßt sich iterieren, wenn für jede Nichteinheit eine zu extrahierende Nichteinheit markiert wird. Um die gewünschte lokale Eindeutigkeit zu erreichen, erweist sich der folgende Begriff als zweckmäßig.

Definition. Eine Abbildung $\mu: S\backslash U \longrightarrow S\backslash U$ heißt eine **Markierung** auf S, wenn
(a) $\mu(x)$ Komponente von x ist, für jedes x
(b) x Komponente von y, $\mu(y)$ Komponente von x impliziert, daß $\mu(x) = \mu(y)$.
Ist μ eine Markierung auf S, dann heißt die Abbildung $e: S\backslash U \longrightarrow S$, definiert durch $e(x) = e(\mu(x), x)$,
markierte Extraktion auf S.

Lemma 1. Für $x \in S\backslash U$, S Extraktionsbereich, sei $m(x) = \sup\{i \in \mathbb{N} \cup \{0\} \mid e^i(x) \in S\backslash U\}$
$x_i = e^i(x)$, $e_i = \mu(x_i)$ und $x_i^{n_i} = e_i^{m_i} e(e_i, x_i)$ für $0 \leqq i < m(x)+1$.

Die Folgen der x_i und e_i haben folgende Eigenschaften:
Für $0 \leqq i \leqq j < m(x)+1$ ist
(a) $x_i^{k_i} = e_i^{l_i} \cdot e_{i+1}^{l_{i+1}} \ldots e_j^{l_j} \cdot x_{j+1}$
mit $k_i = n_i \cdot n_{i+1} \ldots n_j \in \mathbb{N}$, $l_i = m_i \cdot n_{i+1} \ldots n_j \in \mathbb{N}$.
(b) $\mathrm{rad}(x_i) \subsetneqq \mathrm{rad}(x_{i+1})$, und e_i ist Komponente von x_i, aber nicht von x_{i+1}. Insbesondere sind e_i und e_j nicht assoziiert für $i \neq j$.

Beweis:
(a) Nach Definition ist $x_{i+1} = e(x_i) = e(\mu(x_i), x_i) = e(e_i, x_i)$, also $x_i^{n_i} = e_i^{m_i} \cdot x_{i+1}$. Durch Iteration folgt (a), wobei $l_i \in \mathbb{N}$, da $\mu(x_i)$ Komponente von x_i ist.
(b) Nach (a) ist $\mathrm{rad}(x_i) = \mathrm{rad}(e_i) \cap \mathrm{rad}(e_{i+1}) \ldots \cap \mathrm{rad}(e_j) \cap \mathrm{rad}(x_{j+1})$, also $\mathrm{rad}(x_i) \subset \subset \mathrm{rad}(x_{i+1})$. Wegen $x_i^{n_i} = e_i^{m_i} \cdot x_{i+1}$ ist $\lambda(e_i, x_{i+1}) = 0$, also e_i keine Komponente von x_{i+1}, also $x_{i+1} \notin \mathrm{rad}(e_i)$. Da $e_i = \mu(x_i)$ Komponente von x_i, so $x_i \in \mathrm{rad}(e_i)$. Also ist $\mathrm{rad}(x_i) \neq \mathrm{rad}(x_{i+1})$. Wären für $i < j$ e_i und e_j assoziiert, so $\mathrm{rad}(x_{i+1}) \subset \mathrm{rad}(x_j) \subset \subset \mathrm{rad}(e_j) = \mathrm{rad}(e_i)$, also wäre e_i eine Komponente von x_{i+1}.

Der durch Iteration der markierten Extraktion definierte **Extraktionsalgorithmus** bricht wegen Lemma 1(b) nach endlich vielen Schritten ab, wenn S der folgenden Endlichkeitsbedingung genügt.

Definition. Ein Bereich S heißt vom **endlichen Typ,** wenn jede aufsteigende Kette $\mathrm{rad}(y_1) \subset \mathrm{rad}(y_2) \subset \ldots, (y_i \in S)$ konstant wird.

Bemerkungen
(1) Für $y \in S$ sei $F(y) = \{x \in S \mid \lambda(x,y) > 0\}$ die Menge aller Komponenten von y. F(y) ist der kleinste Unterbereich von S, der y enthält und mit jedem Element auch deren Teiler. Es ist $\mathrm{rad}(y) \subset \mathrm{rad}(y')$ genau dann, wenn $F(y) \supset F(y')$. Daher ist ein Bereich S genau dann vom endlichen Typ, wenn jede absteigende Kette von Komponentenmengen $F(\cdot)$ konstant wird.

(2) Ist R ein Krullring, so ist R* vom endlichen Typ, denn nach Folgerung (2) von Abschnitt 1 gilt $\mathrm{rad}(y)\subset\mathrm{rad}(x) \Leftrightarrow \lambda(x,y)>0 \Leftrightarrow \{i\in I \mid v_i(x)>0\}\subset\{i\in I \mid v_i(y)>0\}$ und letztere Indexmengen sind endlich.
Offensichtlich ist für einen noetherschen Ring R der Bereich R* vom endlichen Typ, die Umkehrung gilt jedoch nicht (da nicht jeder Krullring noethersch ist).

(3) Ist $h: S\longrightarrow R$ ein Halbgruppenhomomorphismus der Bereiche S und R mit $h(x)\mid_R h(y) \Leftrightarrow x\mid_S y$ für $x,y\in S$, so ist mit R auch S vom endlichen Typ.
Insbesondere sind also Bereiche mit Divisorentheorie vom endlichen Typ.

Ist S ein Extraktionsbereich vom endlichen Typ, so erzeugt der Extraktionsalgorithmus nach Lemma 1 eine endliche Folge (e_i), die μ-unabhängig in folgendem Sinne ist.

Definition. Eine endliche Menge von nichtassoziierten Nichteinheiten in einem Extraktionsbereich S mit Markierung μ heißt μ-**unabhängig,** wenn Nichteinheiten $y_0,y_1,\ldots,y_m$ existieren, so daß $M=\{\mu(y_0),\mu(y_1),\ldots,\mu(y_m)\}$ und $\mathrm{rad}(y_0)\subset\mathrm{rad}(y_1)\subset\ldots\subset\mathrm{rad}(y_m)$. (Die Mengen dieser Kette sind dann verschieden.

Lemma 2. Sei $M=\{a_0,a_1,\ldots,a_m\}$ eine μ-unabhängige Menge im Extraktionsbereich S mit Markierung μ, und

$$x = a_0^{r_0}\cdot a_1^{r_1}\ldots a_m^{r_m}\cdot u \text{ mit } r_i\in\mathbb{N},\ u\in U.$$

Der Extraktionsalgorithmus angewandt auf x ergibt (vgl. Lemma 1): $m(x)=m$, $a_i=e_i$ für $0\leqq i\leqq m$, und

$$r_i=\frac{m_i}{n_0n_1\ldots n_i} \quad \text{wobei} \quad x_i^{n_i}=e_i^{m_i}\cdot e(e_i,x_i).$$

Beweis: Es ist $\mathrm{rad}(x)=\mathrm{rad}(a_0)\cap\mathrm{rad}(a_1)\cap\ldots\cap\mathrm{rad}(a_m)$. Da $a_i=\mu(y_i)$ mit $\mathrm{rad}(y_0)\subset\ldots\subset\mathrm{rad}(y_m)$, so ist a_i Komponente von y_i, also $\mathrm{rad}(y_i)\subset\mathrm{rad}(a_i)$, und daher $y_0\in\mathrm{rad}(x)$. Also ist x Komponente von y_0. Da $a_0=\mu(y_0)$ Komponente von x, so ist nach Definition der Markierung $a_0=\mu(y_0)=\mu(x)=e_0$.

Es ist $\lambda(a_0,x)=\frac{m_0}{n_0}\geqq r_0$, $x^{n_0}=a_0^{m_0}\cdot e(a_0,x)$. Also $a_0^{m_0-n_0r_0}\cdot e(a_0,x)=a_1^{r_1n_0}\ldots a_m^{r_mn_0}u^{n_0}$.

Wäre $m_0-n_0r_0>0$, so $\mathrm{rad}(a_1)\cap\mathrm{rad}(a_2)\cap\ldots\cap\mathrm{rad}(a_m)\subset\mathrm{rad}(a_0)$, also $\mathrm{rad}(y_1)\subset\mathrm{rad}(a_0)$ und daher a_0 Komponente von y_1. Da y_1 Komponente von y_0, so wäre nach Definition der Markierung $a_1=\mu(y_1)=\mu(y_0)=a_0$, und M wäre nicht μ-unabhängig. Also ist $m_0-n_0r_0=0$. Damit

$r_0=\frac{m_0}{n_0}$ wobei $x_0^{n_0}=e_0^{m_0}\cdot e(e_0,x_0)$, und
$x_1=e(a_0,x)=a_1^{r_1n_0}\ldots a_m^{r_mn_0}u^{n_0}$. Durch Iteration dieses Arguments für $x_1,x_2,\ldots$ folgt das Lemma.

Durch Kombination der beiden Lemmata ergibt sich der folgende Satz.

Satz 2 (markierte Faktorisierung)
Sei S ein Extraktionsbereich vom endlichen Typ, versehen mit einer Markierung μ. Dann hat jede Nichteinheit

x von S eine Darstellung $\quad x^n=u\prod_{a\in M}a^{n_a}$

mit eindeutig bestimmter μ-unabhängiger Menge M, eindeutig bestimmten Quotienten $\frac{n_s}{n}$ positiver ganzer Zahlen und mit Einheit u. Diese markierte Faktorisierung wird durch den Extraktionsalgorithmus geliefert.

Es soll nun gezeigt werden, daß ein Extraktionsbereich vom endlichen Typ tatsächlich eine Markierung besitzt.

Definition. Eine Nichteinheit y eines Extraktionsbereiches heiße **extremal,** wenn für jede Nichteinheit x, die y teilt, e(x,y) eine Einheit ist.

Irreduzible Elemente sind stets extremal.

Lemma 3

(a) Ist S ein Extraktionsbereich vom endlichen Typ (nicht nur aus Einheiten bestehend), so hat jede Nichteinheit eine extremale Komponente, und es existiert eine extremale Markierung, d.h. eine Markierung, deren Werte extremale Elemente sind.

(b) Ist S die multiplikative Halbgruppe eines Krullringes, so hat jede Nichteinheit eine irreduzible Komponente, und es existiert eine irreduzible Markierung, d.h. eine Markierung, deren Werte irreduzible Elemente sind.

Beweis:

(a) Sei $y \in S \setminus U$. Es wird gezeigt, daß y eine extremale Komponente hat. Ist y extremal, so ist nichts zu zeigen. Ist y nicht extremal, so gibt es ein $x \in S \setminus U$ mit $x|y$ und $y_1 = e(x,y) \notin U$. Es ist $y^n = x^m \cdot y_1$, $\frac{m}{n} = \lambda(x,y)$, und daher $\mathrm{rad}(y) \subset \mathrm{rad}(y_1)$. Nach Definition von y_1 ist $\lambda(x,y_1) = 0$, also $y_1 \notin \mathrm{rad}(x)$ und daher $y_1 \notin \mathrm{rad}(y)$. Also ist $\mathrm{rad}(y) \subsetneqq \mathrm{rad}(y_1)$. Ist y_1 extremal, so eine extremale Komponente von y. Ist y_1 nicht extremal, so ergibt sich wie eben die Existenz eines $y_2 \notin U$ mit $\mathrm{rad}(y_1) \subsetneqq \mathrm{rad}(y_2)$. Durch Iteration ergibt sich die Existenz einer extremalen Komponente von y, da S vom endlichen Typ ist.

Sei nun M ein Repräsentantensystem, bzgl. Assoziiertsein, der nicht leeren Menge aller extremalen Elemente von S. M sei mit einer beliebigen Wohlordnung „<" versehen. Ist für $x \in S \setminus U$ $\mu(x)$ die bzgl. „<" kleinste Komponente von x aus M, so ist μ eine extremale Markierung auf S.

(b) In einem Krullring wird jede aufsteigende Kette $(y_1) \subset (y_2) \subset \ldots$ konstant, und daher besitzt jede Nichteinheit eine irreduzible Komponente. Analog wie unter (a) ergibt sich die Existenz einer irreduziblen Markierung.

Aus Satz 2 ergibt sich mit Hilfe von Lemma 3 (und früheren Folgerungen bzw. Bemerkungen) das folgende Korollar.

Korollar. Ist S ein Extraktionsbereich von endlichem Typ (z.B. multiplikative Halbgruppe eines Krullringes), so gibt es eine Markierung auf S derart, daß jede Nichteinheit eine eindeutige markierte Faktorisierung im Sinne von Satz 2 in extremale (irreduzible) Elemente hat. Sind alle extremalen (irreduziblen) Elemente semiprim, so kann in der Faktorisierung $n = 1$ gewählt werden.

3. Gauß-Komplexe

Sei S ein Extraktionsbereich mit Markierung μ ($S \neq U$). Für eine Teilmenge $M \subset S$ sei $S(M)$ die von M und U in S erzeugte Halbgruppe. Für einen Bereich B bezeichne $Pr(B)$ bzw. $Ir(B)$ die Menge der Elemente von B, die prim bzw. irreduzibel sind.

Definition. Eine beliebige Teilmenge M von S heiße μ-**unabhängig,** wenn jede endliche Teilmenge von M μ-unabhängig ist. Eine maximale μ-unabhängige Menge heiße **markierte Basis** (μ-Basis).

Nach Zorn's Lemma ist jede μ-unabhängie Menge in einer markierten Basis enthalten.

Lemma 4. Ist μ irreduzibel, so gibt es ein Repräsentantensystem (bzgl. Assoziiertsein) von Pr(S), das μ-unabhängig ist.

Beweis: Ist P eine endliche Teilmenge von Pr(S), so gibt es $u \in U$, $p' \in P$ mit $\mu(\prod_{p \in P} p) = up'$, denn: Ist $x = \prod_{p \in P} p$, so ist $y = \mu(x)$ irreduzibel und eine Komponente von x, also $x^k = y \cdot z$ mit $z \in S$. Teilte kein $p \in P$ das y, so wäre $x^k | z$ und y eine Einheit. Also gibt es ein $p' \in P$ mit $p' | y$. Da y irreduzibel, so $y = up'$ mit $u \in U$. Insbesondere ist also für $p \in Pr(S)$ $\mu(p) = up, u \in U$. Für $\tilde{p} = up$ gilt dann $\mu(\tilde{p}) = \mu(p) = \tilde{p}$. Sei M das Repräsentantensystem der $\tilde{p}$ mit $p \in Pr(S)$. Ist $P \subset M$, P endlich, so nach dem eingangs gezeigten $\mu(\prod_{p \in P} p) = up'$ mit $u \in U, p' \in P$. Da $\mu(\mu(\cdot)) = \mu(\cdot)$, so $\mu(\prod_{p \in P} p) = \mu(up') = \mu(p') = p'$. Setze $p_1 = p'$.

Analog ergibt sich $\mu(\prod_{p \in P \setminus \{p_1\}} p) = p_2$, $p_2 \in P \setminus \{p_1\}$.

Durch Iteration erhält man $P = \{p_1, p_2, \ldots, p_n\}$ mit $\mu(p_i \ldots p_n) = p_i$ für $1 \leqq i \leqq n$. Mit $y_i = p_i \ldots p_n$ folgt $p_i = \mu(y_i)$ und $\mathrm{rad}(y_1) \subset \mathrm{rad}(y_2) \subset \ldots \subset \mathrm{rad}(y_n)$. Also ist P μ-unabhängig und daher auch M.

Lemma 5. Für eine μ-unabhängige Menge M ist S(M) ein Gaußbereich mit $Pr(S(M)) = M \cdot U$. Ist μ irreduzibel, so ist $Pr(S(M)) = Ir(S) \cap S(M)$.

Beweis: Es ist $S(M) = \{u \prod_{a \in M} a^{n_a} | u \in U, n_a \in \mathbb{N}$ für endlich viele a, sonst $0\}$. Also ist $Pr(S(M)) \subset M \cdot U$ und $M \cdot U = Ir(S) \cap S(M)$, wenn μ irreduzibel ist. Es genügt daher, zu zeigen, daß $M \subset Pr(S(M))$ ist. Sei $a_0 \in M$, und zunächst $a_0 | u \prod_{a \in M} a^{n_a}$ in S(M). Also $u \prod_{a \in M} a^{n_a} = a_0 \cdot v \prod_{a \in M} a^{m_a}$, wobei $u, v \in U$ und nur endlich viele $n_a, m_a \in \mathbb{N}$. Aus der Eindeutigkeitsaussage von Lemma 2 folgt $n_{a_0} > 0$. Sei nun $a_0 | x \cdot y$ mit $x = u \prod_{a \in M} a^{k_a}$, $y = v \prod_{a \in M} a^{l_a}$ (in S(M)). Nach dem eben Gezeigten ist $k_{a_0} + l_{a_0} > 0$, also $k_{a_0} > 0$ oder $l_{a_0} > 0$ und daher $a_0 | x$ oder $a_0 | y$. Also ist $a_0 \in Pr(S(M))$.

Lemma 6. Sind M und N μ-unabhängige Teilmengen von S, so gilt:

(a) $S(M) \cap S(N) = S(M \cap N)$

(b) Ist $x^m y^n \in S(M)$ mit $m, n \in \mathbb{N}$, so ist mit $x, y \in S(N)$ auch $x, y \in S(M)$.

Beweis:

(a) Es ist $S(M \cap N) \subset S(M) \cap S(N)$. Sei $x \in S(M) \cap S(N)$, also $x = u \prod_{a \in M} a^{n_a} = v \prod_{b \in N} b^{m_b}$ mit $u, v \in U$ und $n_a, m_b \in \mathbb{N}$ nur für endlich viele a bzw. b. Nach Lemma 2 ist $\{a \in M | n_a \in \mathbb{N}\} = \{b \in N | n_b \in \mathbb{N}\}$, also $x \in S(M \cap N)$.

(b) Seien $x,y \in S(N)$, also $x = u\prod_{b\in N} b^{m_b}$, $y = v\cdot\prod_{b\in N} b^{n_b}$ $m_b,n_b \in \mathbb{N}$ nur für endlich viele $b\in\mathbb{N}$. Ist $x^m y^n \in S(M)$, so $u^m v^n \prod_{b\in N} b^{mm_b+nn_b} = w\prod_{a\in M} a^{n_a}$. Ist $m,n\in\mathbb{N}$ und $m_b\in\mathbb{N}$ oder $n_b\in\mathbb{N}$, so $mm_b+nn_b\in\mathbb{N}$, also nach Lemma 2 $b\in M$. Damit $x\in S(M)$ und $y\in S(M)$.

Definition. Die nichtleere Familie

$\mathfrak{G} = \{S(M) | M$ markierte Basis von $S\}$ heiße

Gauß-Komplex von S bzgl. μ.

Aus den Lemmata 5 und 6 und Satz 2 (bzw. des Korollars dazu) ergibt sich

Satz 3. Ist S ein Extraktionsbereich vom endlichen Typ mit einer irreduziblen Markierung, ist insbesondere S die multiplikative Halbgruppe eines Krullbereichs, so hat der Gauß-Komplex von S folgende Eigenschaften:

(a) Jedes $G\in\mathfrak{G}$ ist ein Gaußbereich, maximal in $\mathfrak{G}$.

(b) $Pr(G) = Ir(S)\cap G$ für $G\in\mathfrak{G}$.

(c) Für $G,G'\in\mathfrak{G}$ ist $G\cap G'$ wieder ein Gaußbereich, dessen Teilbarkeitsrelation auf $G\cap G'$ mit der von G und G' übereinstimmt und für den $Pr(G\cap G') = Pr(G)\cap \cap Pr(G')$ gilt.

(d) Für jedes Element von S liegt eine Potenz in $\bigcup_{G\in\mathfrak{G}} G$.

Faktorielle Ringe (Gaußringe) lassen sich folgendermaßen durch einen einfachen Gauß-Komplex charakterisieren.

Korollar. Folgende Aussagen für einen Ring R sind äquivalent.

(a) R ist faktoriell.

(b) R ist ein Krullring, dessen irreduzible Elemente semiprim sind und dessen Gauß-Komplex für jede irreduzible Markierung einelementig ist.

(c) R^* ist ein Extraktionsbereich vom endlichen Typ, und es existiert eine irreduzible Markierung, so daß der zugehörige Gauß-Komplex ganz R^* überdeckt und einelementig ist.

Beweis:

(a) $\Rightarrow$ (b): Ist R faktoriell, so ist R ein Krullring, dessen irreduzible Elemente prim, also semiprim sind. Ist μ eine irreduzible Markierung auf R^*, so gibt es nach Lemma 4 ein Repräsentantensystem M von $Pr(R^*)$, das μ-unabhängig ist. Also $S(M)\subset G\in\mathfrak{G}$, wobei $\mathfrak{G}$ der Gauß-Komplex bzgl. μ ist. Da $S = S(M)\subset G$, so $S = G$. Wegen der Maximalität aller $G\in\mathfrak{G}$ ist also $\mathfrak{G} = \{S\}$, also $\mathfrak{G}$ einelementig.

(b) $\Rightarrow$ (c): Da R Krullring, so ist R^* ein Extraktionsbereich vom endlichen Typ. Nach Lemma 3 gibt es eine irreduzible Markierung auf R^*. Nach Voraussetzung ist der zugehörige Gauß-Komplex einelementig. Da jedes irreduzible Element semiprim ist, so überdeckt der Gauß-Komplex ganz R^*.

(c) $\Rightarrow$ (a): Aus (c) folgt, daß R^* ein Gaußbereich ist, also R faktoriell.

Bemerkung. Das Korollar legt nahe, als den Gaußbereichen benachbart, solche Bereiche anzusehen, deren Gauß-Komplex bezüglich einer geeigneten Markierung nur

aus einem einzigen Gaußbereich besteht. Ist S ein solcher **quasi-Gaußbereich** mit $\mathfrak{G} = \{G\}$ für eine geeignete Markierung, so ist G ein gaußscher Unterbereich von S, dessen Teilbarkeitsrelation mit der von S übereinstimmt und für den gilt $S = \mathrm{rad}G = \{x \in S | x^n \in G \text{ für ein } n \in \mathbb{N}\}$. Es zeigt sich, daß umgekehrt ein Extraktionsbereich vom endlichen Typ S, der einen Gaußbereich G enthält, dessen Teilbarkeitsrelation mit der von S übereinstimmt und für den $S = \mathrm{rad}G$ gilt, ein quasi-Gaußbereich ist. So gesehen ist ein quasi-Gaußbereich, ohne daß ideale Elemente eingeführt würden, ein Pendant zu einem Bereich mit Divisorentheorie, dessen Divisorenklassenhalbgruppe eine Torsionshalbgruppe ist; letztere sind in der Tat quasi-Gaußbereiche. Ein quasi-Gaußbereich läßt sich auch charakterisieren als ein Extraktionsbereich vom endlichen Typ S, in dem von jeder Nichteinheit eine geeignete Potenz Produkt von quasiprimen Elementen ist; dabei heißt eine Nichteinheit quasiprim, wenn $\lambda(x, \cdot)$ additiv auf S ist. Ist insbesondere S die multiplikative Halbgruppe eines Krullringes R, so sind die quasiprimen Elemente gerade die primären Elemente, d.h. diejenigen, die ein primäres Ideal erzeugen. Es ist S genau dann ein quasi-Gaußbereich, wenn R fastfaktoriell ist (vgl. [Storch]).

Literatur

Bourbaki, N.: Commutative Algebra. Chapter VII Divisors. Hermann, Paris 1972.

Greiter, G.: Nonunique factorization in subsemigroups of semigroups with unique prime factorization. American Mathematical Monthly, 1980, p. 473–474.

Gundlach, K.B.: Einführung in die Zahlentheorie. Bibliographisches Institut, Mannheim 1972.

Hinrichsen, D. / Krause, U.: Unique representation in convex sets by extraction of marked components. Forschungsschwerpunkt Dynamische Systeme, Report Nr. 48, Bremen 1981.

Kuroš, A.G.: Vorlesungen über allgemeine Algebra. Teubner, Leipzig 1964.

Sommer, J.: Vorlesungen über Zahlentheorie. Teubner, Leipzig und Berlin 1907.

Storch, U.: Fastfaktorielle Ringe. Schriftenreihe des Mathematischen Instituts der Universität Münster, Heft 36, 1967.